

provided with the SNMP manager, a source IP address
of the managing computer 4 is stored in the
intelligent interconnecting device 1 as managing
apparatus information in order to limit a
5 transmission destination of an event notice (Trap)
from the intelligent interconnecting device 1 to
a specific computer, for example, only the managing
computer 4 so that the Trap is transmitted only to
the managing computer 4 and thereby careless spread
10 of information can be prevented.

【0029】 Furthermore, the authentication
processing in the steps S110, S112 in FIG. 3 and
FIG. 4 may be, for example, enciphered to improve
security.

15 The explanation of the above structure example
is made on the premise that the unauthorized access
avoiding program for an intelligent
interconnecting device to be executed by the
central controlling section 6 is stored in a
20 nonvolatile semiconductor memory constituting a
part of the storage section 9 which works as a
recoding medium of the program and is executed by
being read in the central controlling section 6
from the semiconductor memory, but the use of the
25 semiconductor memory is not of course restrictive.

More specifically, a flexible disk, a CD-ROM,
an optical recording medium such as a DVD and a PD,
a magneto-optic recording medium such as an MD, a
magnetic recording medium, and the like may be used
5 as a recording medium other than the semiconductor
memory. Incidentally, special apparatus for
reading and writing data are required for some of
these recording media and the storage section 9 may
of course be constituted by including these
10 apparatus.

[0030] As described above, according to the
present invention, the source IP address of the
managing computer is extracted and stored from a
packet which is received through the execution
15 processing of the existing TCP/IP protocol and
communication with an external apparatus having an
IP address other than the stored source IP address
is not allowed thereafter, which brings about an
effect that security, which is not sufficiently
20 secured in a conventional authentication
processing by the TCP/IP protocol, is further
improved and a system with high reliability can be
provided compared with a conventional example.

Moreover, the authentication processing by
25 the TCP/IP protocol is carried out after the source

IP address is judged to be identical with the stored
source IP address and therefore, sufficient
security is maintained in an intelligent
interconnecting device in which TCP/IP protocols
5 of various kinds are provided by executing the
authentication processing by one of these
protocols. Thereby, the authentication
processing by the individual protocols can be
omitted. This brings about an effect that software
10 load can be reduced.

[0031] Furthermore, a response to an access by
a broadcast can be restricted. This makes it
difficult for an outside intruder to recognize the
existence of an apparatus to be managed, in other
15 words, the intelligent interconnecting device to
be managed by the managing computer, so that
security is further improved compared with the
conventional example.

In addition, the user identifier and the
20 password, which are conventionally prepared for
each protocol, can be integrated. This brings
about an effect that software is allowed to be
simplified.